اب جینز میں میل ویئر (malware) نصب کرکے کمپیوٹر پروگراموں کو نشانہ بنایا جاسکتا ہے۔

ریسرچرز کی ایک ٹیم نے ڈی این اے کی مدد سے سافٹ ویئر کو ہیک کرنے کے بعد دعویٰ کیا ہے کہ وہ ایک جینیاتی مالیکیول میں نصب میل ویئر(Malware) کے ذریعے ایک کمپیوٹر پر کنٹرول حاصل کرنے میں کامیاب ہوگئے ہیں۔

اس حیاتیاتی میل ویئر(Malware) کو یونیورسٹی آف واشنگٹن سیٹل کے سائنسدانوں نے تیار کیا ہے، اور اسے "دنیا کا پہلا ڈی این اے استعمال کرنے والا کمپیوٹر ہیکنگ سسٹم" کہا جارہا ہے۔

اس ہیک کے لیے ٹاڈایوشی کوہنو (Tadayoshi Kohno) اور لویس سیزے (Luis Ceze) کی سربراہی میں ایک ٹیم نے آن لائن خریدے جانے والے ڈی این اے میں نقصان دہ سافٹ ویئر کی اینکوڈنگ کی۔ اس کے بعد انھوں نے اس ڈی این اے کو ایک سیکوینسنگ مشین سے گزارا، اور پھر اسے پراسیسنگ کے لیے ایک اور کمپیوٹر کی جانب بھیجا، جس پر ریسرچرز نے قبضہ کرنے کی کوشش کی۔

ریسرچرز تنبیہہ کرتے ہیں کہ ہیکرز کسی دن جعلی خون یا تھوک کے سیمپلز کی مدد سے کسی یونیورسٹی کے کمپیوٹرز میں زبردستی گھسنے، پولیس کے فورینزک لیبس کی معلومات چوری کرنے یا سائنسدانوں کی جینوم کی فائلوں میں انفیکشن متعارف کرنے کی کوشش کرسکتے ہیں۔

اس وقت ڈی این اے کے ذریعے میل ویئر(Malware) پھیلنے کا زیادہ خطرہ نہیں ہے۔ ریسرچرز اعتراف کرتے ہیں کہ انھوں نے سیکورٹی فیچرز غیرفعال کرکے اور ایک بائیوانفارمیٹکس پروگرام کو کھلا رکھ کر اپنے تجربے کی کامیابی کے امکانات میں اضافہ کیا تھا۔ MyHeritage.com نامی علم الانساب (genealogy) کی ویب سائٹ کے چیف سائنٹیفک افسر، جیناتی ماہر اور پروگرامر یانیو

ایرلخ (Yaniv Erlich) کہتے ہیں کہ ان سائنسدانوں کے تجربے کو اس وقت عملی جامہ نہیں پہنایا جاسکتا ہے۔

ماضی میں کوہنو نے ایک گاڑی کے پورٹ میں ہیک کرکے بلیوٹوتھ کنکشنز کے ذریعے حملے کرکے ریموٹ طریقے سے قبضہ حاصل کرنے کی بھی کوشش کی تھی۔

ڈی این اے استعمال کرنے والے اس میل ویئر(Malware) کو وینکوور میں منعقد ہونے والے یوزنکس سیکورٹی سپموزیم(Usenix Security Symposium) میں پیش کیا جائے گا۔ کوہنو کے سیکورٹی اور پرائویسی ریسرچ لیب کے طالب علم پیٹر نے (Peter Ney) کہتے ہیں "ہم ابھرتی ہوئی ٹیکنالوجیز پر حملوں کی پیشگوئی کرنے کی کوشش کرتے ہیں، تاکہ ان کے پیشگی توڑ تلاش کیے جاسکیں۔"

میل ویئر(Malware) تخلیق کرنے کے لیے ریسرچرز کی ٹیم نے ایک کمپیوٹر کے کمانڈ کو 176 ڈی این اے کے حروف A، G، C اور T میں تبدیل کیا۔ انھوں نے 89 ڈالر کے عوض ڈی این اے خریدنے کے بعد، اسے ایک سیکوینسنگ مشین میں ڈالا، جس نے جین کے حروف پڑھنے کے بعد انھیں 0 اور 1 کی شکل میں سٹور کیا۔

ارلخ کہتے ہیں کہ انھوں نے "سپل اوور (spillover)" کا فائدہ اٹھایا ہے، جس میں سٹوریج کے بفر سے تجاوز ہونے والے ڈیٹا کی تشریح کمپیوٹر کمانڈ کے طور پر کی جاتی ہے۔ اس کمانڈ نے ایک سرور سے رابطہ کیا، جس پر کوہنو کی ٹیم نے کنٹرول حاصل کیا ہوا تھا، اور اس کے بعد یہ ٹیم اپنی لیب کے اس کمپیوٹر پر کنٹرول حاصل کرنے میں کامیاب ہوگئی، جسے ڈی این اے کی فائل کے تجزیے کے لیے استعمال کیا جارہا تھا۔

سائنسدانوں کو مصنوعی ڈی این اے کے سٹرانڈز بنانے والی کمپنیاں بائیودہشت گردوں کے سلسلے میں محتاط ہیں۔ ریسرچرز کہتے ہیں کہ مستقبل میں انھیں ڈی این اے کی مدد سے کمپیوٹر کی ہیکننگ پر بھی نظر رکھنے کی ضرورت ہوگی۔

یونیورسٹی آف واشنگٹن کی ٹیم یہ بھی تنبیہہ کرتی ہے کہ جینیاتی ڈیٹا انٹرنیٹ اور ایپس پر زیادہ آسانی سے دستیاب ہے، جس کی وجہ سے ہیکرز رواتی انداز سے بھی اسے نشانہ بنا سکتے ہیں۔

مملکت متحدہ کے سینگر انسٹی ٹیوٹ (Sanger Institute) میں بائیوانفارمیٹکس کے ماہر جیمز بون فیلڈ (James Bonfield)کہتے ہیں کہ بعض دفعہ ڈی این اے کے ڈیٹا کو منظم کرنے اور اس کی تشریح کرنے والے سائنٹیفک پروگرامز کو برقرار نہیں رکھا جاتا ہے، جس کی وجہ سے انھیں نشانہ بنانا زیادہ آسان ہوجاتا ہے۔ بون فیلڈ کہتے ہیں کہ جس پروگرام کو یونیورسٹی آف واشنگٹن کے ریسرچرز نے نشانہ بنایا تھا، اس کے مصنف وہ خود تھے۔ وہ بتاتے ہیں کہ یہ پروگرام، جس کا نام fqzcomp تھا، ایک مقابلے کے لیے تیار کیا گیا تھا، اور ان کے اندازے کے مطابق اسے کبھی استعمال میں نہیں لایا گیا تھا۔

تحریر: انٹونیو ریگالوڈو (Antonio Regalado)